Department of Homeland Security Daily Open Source Infrastructure Report for 02 April 2007

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports that the Transportation Security Administration, FBI, and other law enforcement agencies are investigating how a concealed handgun carried by a flight attendant passed through security unnoticed in Atlanta. (See item 8)
- US−CERT has released Technical Cyber Security Alert TA07−089A: Microsoft Windows ANI header stack buffer overflow (See item 26)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *April 01, New York Times* — **Security agency computers missing.** The office in charge of protecting American technical secrets about nuclear weapons from foreign spies is missing 20 desktop computers, at least 14 of which have been used for classified information, the Department of Energy (DOE) inspector general reported Friday, March 30. This is the 13th time in a little over four years that an audit has found the department, whose national laboratories and factories do most of the work in designing and building nuclear warheads, has lost control over computers used in working on the bombs. "Problems with the control and accountability of desktop and laptop computers have plagued the department for a number of years," the report said. In January, Linton F. Brooks was fired as the administrator of the

National Nuclear Security Agency, the DOE agency in charge of bombs, because of security problems. Previous incidents of wayward computers have involved nuclear−weapons information. But the office involved in this breach has a special responsibility, tracking and countering efforts to steal bomb information. Its computers would have material on what the department knew about foreign operatives and efforts to steal sensitive information.
Source: http://www.mercurynews.com/politics/ci_5569889?nclick_check= 1

2. *March 31, Bloomberg* — **Marseille Union, Gaz de France to end port strike affecting LNG supply flow.** Marseille port workers voted to end a 17−day old strike at a Gaz de France SA terminal that has 63 vessels stranded outside Europe's second−largest oil−import hub. The port workers union and the company reached an agreement late Friday, March 30, said Pascal Galeote of the Confédération Générale du Travail (CGT). The agreement allowed port operations to resume from Saturday afternoon, restoring the flow of supplies to refineries and chemical factories. The strike was started by the CGT over the future of the workforce at a liquefied natural gas terminal that is under construction at Fos by Gaz de France. The company planned to use its own employees to load and unload LNG tankers at the terminal, which is scheduled to open by the end of this year. Gaz de France had said it was necessary for the LNG tankers to be unloaded by its own personnel for safety reasons. The strike, which began March 14, has cost refining and petrochemical companies tens of millions of euros so far and may be boosting gasoline prices in New York.
Source: http://www.bloomberg.com/apps/news?pid=20601072&sid=a93LnwH7KDL4&refer=energy

3. *March 29, Associated Press* — **BP may reverse U.S.−Canada pipeline.** BP PLC on Thursday, March 29, said it will consider reversing a pipeline to deliver Canadian crude oil to Oklahoma and would offer discounted capacity to shippers willing to make long−term contracts. The 600−mile pipeline could be flowing southbound by mid−2009, BP said, and would transport light Canadian crude oil to Cushing, OK, a major oil hub −− provided shippers show adequate interest in the project. BP expects the pipeline to have capacity to carry 100,000 barrels per day. Future expansions could boost daily capacity to 200,000 barrels.
Source: http://www.businessweek.com/ap/financialnews/D8O61BVG0.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4. *March 30, Government Accountability Office* — **GAO−07−406SP: Defense Acquisitions: Assessments of Selected Weapon Programs.** The Government Accountability Office (GAO) assessed 62 weapon systems with a total investment of over $950 billion, some two−thirds of the $1.5 trillion Department of Defense (DoD) plans for weapons acquisition. Several of these programs will be developed without needed technology, design, and production knowledge, and

will cost more and take longer to deliver. Limited progress has been made by the programs GAO assessed. Fully mature technologies were present in 16 percent of the systems at development start −− the point at which best practices indicate mature levels should be present. The programs that began development with immature technologies experienced a 32.3 percent cost increase, whereas those that began with mature technologies increased 2.6 percent. Furthermore, 27 percent of the assessed programs demonstrated a stable design at the time of design review and in terms of production, very few programs reported using statistical process control data to measure the maturity of production processes. DoD does not have an environment that facilitates effective program management. Further, DoD is increasingly relying on contractors to perform key management functions raising questions about the capacity of DoD to manage new weapon system programs.
Highlights: http://www.gao.gov/highlights/d07406sphigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−406SP

5. *March 30, Government Accountability Office* — **GAO−07−388: Best Practices: An Integrated Portfolio Management Approach to Weapon System Investments Could Improve DoD's Acquisition Outcomes.** The Government Accountability Office (GAO) was asked to examine how the Department of Defense's (DoD) processes for determining needs and allocating resources can better support weapon system program stability. Specifically, GAO compared DoD's processes for investing in weapon systems to the best practices that successful commercial companies use to achieve a balanced mix of new products, and identified areas where DOD can do better. In conducting its work, GAO identified the best practices of: Caterpillar, Eli Lilly, IBM, Motorola, and Procter and Gamble. GAO is making several recommendations for DoD to implement an integrated portfolio management approach to weapon system investments. DoD stated that it is undertaking several pilot efforts to improve the department's approach and that implementation of any new business rules will be contingent upon the outcomes of these efforts.
Highlights: http://www.gao.gov/highlights/d07388high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−388

6. *March 29, Department of Defense* — **Budget will recapitalize, modernize U.S. forces.** The proposed defense budget will modernize and recapitalize the armed forces, Defense Secretary Robert M. Gates told the House Appropriations Defense Subcommittee Thursday, March 29. Gates said the proposed budget and the emergency supplemental request will exceed $700 billion. The military needs this money to sustain the force, modernize weapons systems, train forces and build defense capabilities. Marine Gen. Peter Pace told the representatives that the heavy demand on U.S. forces is unlikely to dissipate in the near future.
Source: http://www.defenselink.mil/news/newsarticle.aspx?id=32632

[Return to top]

Banking and Finance Sector

7. *March 30, Government Accountability Office* — **GAO−07−364: Information Security: Further Efforts Needed to Address Significant Weaknesses at the Internal Revenue Service.** As part of its audit of the Internal Revenue Service's (IRS) fiscal years 2006 and 2005 financial statements, the Government Accountability Office (GAO) assessed (1) IRS's actions

to correct previously reported information security weaknesses and (2) whether controls were effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. IRS has made limited progress toward correcting or mitigating previously reported information security weaknesses at two data processing sites, but 66 percent of the weaknesses that GAO had previously identified still existed. Specifically, IRS has corrected or mitigated 25 of the 73 information security weaknesses that GAO reported as unresolved at the time of the last review. Significant weaknesses in access controls and other information security controls continue to threaten the confidentiality, integrity, and availability of IRS's financial and tax processing systems and information. A primary reason for the new and old weaknesses is that IRS has not yet fully implemented its information security program. IRS has taken a number of steps to develop, document, and implement an information security program. However, the agency has not yet fully or consistently implemented critical elements of its program.
Highlights: http://www.gao.gov/highlights/d07364high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−364

[Return to top]

Transportation and Border Security Sector

8. *March 31, Associated Press* — **TSA: Attendant brought gun on flight.** A uniformed flight attendant was arrested at Dulles International Airport in Washington, D.C., after she turned herself in for allegedly carrying a concealed handgun aboard a flight from Atlanta, GA, authorities said Saturday, March 31. The Transportation Security Administration (TSA), the FBI, and other law enforcement agencies were investigating how the gun passed through security unnoticed in Atlanta, TSA spokesperson Barry Phelps said. Flight attendants have to go through the same security procedures as all other passengers, he said.
Source: http://www.usatoday.com/travel/news/2007−03−31−tsa−dulles_N. htm

9. *March 31, Aero−News* — **TSA screeners fail tests at Denver International Airport.** Security screeners at Denver International Airport in Denver, CO, have some explaining to do. Last month, Transportation Security Administration (TSA) screeners failed to find simulated weapons and explosive materials carried through by undercover agents roughly nine times out of 10. And they can't blame the equipment. According to Denver's KUSA−9, alarms sounded on screening machines when they encountered suspect devices, just as they're supposed to −− but screeners failed to then follow standard procedures, such as hand−searching luggage and conducting closer inspections of suspect passengers. Items used in the tests included liquid explosives and weapons inside carry−on luggage. In one case, an agent even taped an improvised explosive device to her leg... and convinced the screener it was a bandage from surgery, despite the alarms wailing in the background.
Source: http://www.aero−news.net/index.cfm?ContentBlockID=f7841158−0973−42df−90f4−78388f3d7340&

10. *March 30, Associated Press* — **Bomb hoax forces cruise ship evacuation.** A phony bomb threat forced nearly 3,000 passengers and crew members to evacuate a Carnival Cruise Lines ship shortly before it was scheduled to leave Florida for the Bahamas. Coast Guard and Brevard County, FL, sheriff's officers spent two hours searching the ship Thursday, March 29, before

determining the threat was a hoax. The company released a statement about the incident saying, "Carnival Cruise Lines takes any security threat very seriously and is working with law enforcement officials as the investigation continues."
Source: http://apnews.myway.com/article/20070330/D8O6F45O0.html

11. *March 29, Associated Press* — **Jet without nose landing gear lands safely.** A plane with malfunctioning landing gear touched down safely at Orlando Sanford International Airport in Florida on Thursday afternoon, March 29, officials said. The Allegiant Air flight from Portsmouth, NH, landed without its nose landing gear. None of the 157 passengers on board were injured during the landing, Federal Aviation Administration spokespeson Kathleen Bergen said.
Source: http://www.usatoday.com/news/nation/2007−03−29−emergency−landing_N.htm?POE=NEWISVA

12. *March 29, Associated Press* — **FAA defends outsourced plane repairs.** Aviation regulators on Thursday, March 29, defended U.S. airlines' use of outsourced and overseas plane maintenance shops, saying the number of fatal crashes has declined in recent years even as reliance on these services has increased. "Although the percentage of outsourcing has never been higher, the accident rate has never been lower," Nicholas Sabatini, a top safety official at the Federal Aviation Administration (FAA) told a House subcommittee. "Aviation safety is not dependent on airlines performing their own maintenance." Sabatini also disputed perceptions that use of foreign repair stations is unsafe. Those repair stations, he said, must meet the same standards as those in the United States, or they won't be certified by the FAA. However, the FAA was criticized by some members of Congress for not doing an adequate job of keeping tabs on repair shops, particularly overseas stations without certification from the federal agency.
Source: http://www.chron.com/disp/story.mpl/ap/fn/4672149.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *March 30, Village Soup Citizen (ME)* — **Equine herpes virus confirmed in Maine .** A horse housed in a private stable in Rome, ME, was diagnosed Wednesday, March 28, with the neurologic form of Equine Herpes Virus Type 1 (EHV−1). The three−year−old gelding had been euthanized March 19, 2007, after exhibiting severe neurologic signs over a 24−hour period. A 17−year−old horse at the same location died one day earlier with similar symptoms. According to the State Veterinarian Don Hoenig, this is the first reported case of the neurologic form of EHV−1 in Maine. Additionally, an eight−year−old horse in Wales, previously housed for a short time at the stable in Rome, is under treatment for neurologic signs consistent with EHV−1. The Department of Agriculture has placed both stables under quarantine.

EHV information: http://www.vet.uga.edu/vpp/IVM/ENG/ERD/EHV−4and1.html
Source: http://waldo.villagesoup.com/government/story.cfm?storyID=89 744

[Return to top]

Food Sector

14. *March 30, Reuters* — **Melamine in pet food.** U.S. officials said on Friday, March 30, that melamine, a chemical used in fertilizers in Asia and forbidden in pet food, has been detected in the wheat gluten used by Canada−based Menu Foods. "The association between the melamine in the kidneys and urine of cats that died and the melamine in the food they consumed is undeniable," said Stephen Sundlof, director of the U.S. Food and Drug Administration's (FDA) Center for Veterinary Medicine, during a press conference. Melamine should not be in pet food at all, but its presence has not been confirmed as the cause of sickness or deaths in pets, because there is little research on its effects on those animals, the FDA said. FDA officials said the wheat gluten was imported from China but was not yet known to be used in human food. All wheat gluten coming from there will now be reviewed, they said. On March 16, Menu Foods recalled 60 million cans and pouches of pet food after it was blamed for the deaths of at least 14 animals.
Source: http://ca.today.reuters.com/news/newsArticle.aspx?type=businessNews&storyID=2007−03−30T174212Z_01_WEN5943_RTRIDST_0_BUSINESS−PETFOOD−MELAMINE−COL.XML

15. *March 30, Hartford Courant (CT)* — **Milk contamination occurred at plant.** State agriculture officials say they will look to build in safeguards at the New Britain, CT, plant that produced the contaminated chocolate milk that sickened several Old Saybrook pupils and led to a four−state product recall Wednesday, March 28. Inspectors Thursday, March 29, determined that the contamination occurred at the Guida's Milk & Ice Cream plant when a sanitizing product used to clean machines was not properly rinsed before the milk went through the machine. Officials said the contamination appeared to have been the result of an employee failing to follow procedures, and was limited to one lot of chocolate milk. Old Saybrook police also inspected the Guida plant Thursday and closed the department's investigation into the contamination, which was discovered shortly after lunch began at the Kathleen E. Goodwin elementary school Wednesday. All of the pupils sickened by the milk were feeling better Thursday, school officials said, and all but one had returned to school. The voluntary recall covered 2,200 cases of half−pint, low−fat chocolate milk. According to a statement from the company, approximately 17,750 half−pints were distributed primarily to schools, as well as some hospitals and retailers in New York, Connecticut, Rhode Island and Massachusetts.
Source: http://www.courant.com/news/local/hc−ctbadmilk0330.artmar30,0,12801.story?&track=rss

16. *March 30, USAgNet* — **USDA admits skipped meat plant checks.** For three decades, U.S. inspectors visited 250 meat processing plants as rarely as once every two weeks despite federal law requiring daily inspection, U.S. Department of Agriculture (USDA) officials told lawmakers on Thursday, March 29. "All I can say is, it's been going on for a long time," said Undersecretary Richard Raymond to the House Appropriations subcommittee on agriculture. "It's going to stop now." The practice started under directives issued in the early 1970s, said

Raymond.
Source: http://www.usagnet.com/story−national.php?Id=716&yr=2007

17. *March 30, U.S. Food and Drug Administration* — **Cat food recalled.** Hill's Pet Nutrition, Inc. is voluntarily recalling Prescription Diet m/d Feline dry food from the market. Hill's is taking this precautionary action because during a two−month period in early 2007, wheat gluten for this product was provided by a company that also supplied wheat gluten to Menu Foods. U.S. Food and Drug Administration tests of wheat gluten samples from this period show the presence of a small amount of melamine. This is the only product Hill's currently sells in the U.S. that contains wheat gluten from any supplier. The voluntary recall of Hill's Prescription Diet m/d Feline dry food involves discontinuation of all retail sales and product retrieval from sellers.
Source: http://www.fda.gov/oc/po/firmrecalls/hills303_07.html

18. *March 30, U.S. Food and Drug Administration* — **Canned dog food recalled.** Nestlé Purina PetCare Company announced Friday, March 30, it is voluntarily recalling all sizes and varieties of its ALPO® Prime Cuts in Gravy wet dog food with specific date codes. The Company is taking this voluntary action after learning that wheat gluten containing melamine, a substance not approved for use in food, was provided to Purina by the same company that also supplied Menu Foods. The contamination occurred in a limited production quantity at only one of Purina's 17 pet food manufacturing facilities. Earlier today the U.S. Food and Drug Administration announced the finding of melamine in products related to the March 16 Menu Foods recall, and advised Purina of the source of the contaminated supply.
Source: http://www.fda.gov/oc/po/firmrecalls/purina203_07.html

19. *March 29, Associated Press* — **Judge allows private testing for mad cow.** The federal government must allow meatpackers to test their animals for mad cow disease, a federal judge ruled Thursday, March 29. Creekstone Farms Premium Beef, a meatpacker based in Arkansas City, KS, wants to test all of its cows for the disease, which can be fatal to humans who eat tainted beef. The U.S. Department of Agriculture (USDA) currently regulates the test and administers it to less than one percent of slaughtered cows. The department threatened Creekstone with prosecution if it tested all its animals. U.S. District Judge James Robertson ruled that the government does not have the authority to regulate the test. Robertson put his order on hold until the government can appeal. If the government does not appeal by June 1, he said the ruling would take effect.
Source: http://www.abcnews.go.com/Politics/wireStory?id=2993427

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

20. *April 01, Reuters* — **Egyptian child tests positive for bird flu.** A third Egyptian child has tested positive for the H5N1 bird flu virus, bringing the number of human cases in Egypt to 32, state news agency MENA said on Saturday, March 31. An official with the health ministry said the four−year−old girl came from Qalyoubia province, north of Cairo. Earlier, the health ministry said a four−year−old boy from Qena province, and a seven−year−old boy from Sohag province had been infected with bird flu. The four−year−old girl was admitted to hospital on Friday, March 30, while the two others were admitted on Thursday, March 29.
Source: http://africa.reuters.com/top/news/usnBAN131117.html

21. *March 29, Agence France−Presse* — **Kuwait to cull chickens over bird flu.** Kuwait has ordered the culling of about 1.1 million chickens in a bid to fight an outbreak of bird flu, an official was quoted as saying on Thursday, March 29. The head of the agriculture authority, Jassem al−Bader, told Al−Siyyassah newspaper the culling will take place "in the coming few days" at farms owned by three major companies. The farms are located in Wafra, south of Kuwait City on the Saudi border, where most of the 57 cases of H5N1 virus have been detected since the outbreak was announced on February 25. Since the outbreak began, authorities have culled close to 200,000 fowls which were in contact with infected birds. No human case had been detected.
Source: http://news.yahoo.com/s/afp/20070329/wl_mideast_afp/healthflukuwait_070329163913;_ylt=AusA4Er1YqGv3AAwULGOiUGJOrgF

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

22. *March 30, Government Accountability Office* — **GAO−07−411: Emergency Preparedness: Current Emergency Alert System Has Limitations, and Development of a New Integrated System Will Be Challenging.** During emergencies, the public needs accurate and timely information. Through the Emergency Alert System (EAS), the media play a pivotal role, assisting emergency management personnel in communicating to the public. The Government Accountability Office (GAO) reviewed (1) the media's ability to meet federal requirements for participating in EAS, (2) stakeholder views on the challenges facing EAS and potential changes to it, and (3) the progress made toward developing an integrated alert system. GAO reviewed the Federal Communications Commission's (FCC) proposed rulemaking on EAS and interviewed media outlets, state emergency management officials, and federal agencies responsible for EAS, including FCC and the Federal Emergency Management Agency (FEMA), within the Department of Homeland Security (DHS). To improve the media's ability to issue emergency alerts, GAO recommends that DHS and FCC develop a plan to verify (1) the dependability and effectiveness of the EAS relay system, and (2) that EAS participants have the training to issue effective EAS alerts. Also, DHS and FCC should establish a forum for stakeholders to address the challenges of implementing an integrated alert system. In response,

DHS agreed with the intent of our recommendations. FCC provided technical comments.
Highlights: http://www.gao.gov/highlights/d07411high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−411

23. *March 30, Federal Emergency Management Agency* — **President declares emergency disaster for Iowa.** The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) Friday, March 30, announced that federal disaster aid has been made available for Iowa to supplement state and local recovery efforts in the area struck by record snow and near record snow during the period of February 28 to March 2, 2007. FEMA Director David Paulison said federal funding is available to the state and eligible local governments in the counties of Adair, Audubon, Buena Vista, Carroll, Cass, Clay, Crawford, Emmet, Greene, Guthrie, Hancock, Harrison, Humboldt, Kossuth, Monona, O'Brien, Palo Alto, Pocahontas, Pottawattamie, Sac, Shelby, Winnebago, and Wright.
Source: http://www.fema.gov/news/newsrelease.fema?id=35175

24. *March 29, Department of Homeland Security* — **DHS provides more than $490 million to America's firefighters.** The U.S. Department of Homeland Security (DHS) announced Thursday, March 29, the start of the fiscal year 2007 application period for the Assistance to Firefighters Grant (AFG) program. More than $492.3 million will be awarded this year to fire departments and nonaffiliated emergency management organizations across the nation, bringing the total provided through this program since 2004 to roughly $2.2 billion. "America's firefighters play a pivotal role in keeping our communities safe and our country secure," said Deputy Secretary Michael Jackson. "Local fire departments respond to a wide array of emergencies every day that require special skills, the safest equipment and place responders at great risk of injury and death. The AFG program provides federal resources to supplement local commitments towards ensuring the ability of America's fire service to be ready for the full range of 21st Century risks."
Source: http://www.dhs.gov/xnews/releases/pr_1175180978570.shtm

25. *March 28, Department of Homeland Security* — **DHS establishes TechSolutions program to support emergency response community.** The Department of Homeland Security's (DHS) Science and Technology (S&T) directorate has established a program, TechSolutions, to support the first responder community by accelerating delivery of emerging technologies. TechSolutions is designed to collect technological requirements and provide solutions for first responders. "No one understands the needs of first responders better than first responders," said Jay M. Cohen, Under Secretary for S&T. "Every day, hundreds of law enforcement officers, fire fighters, emergency medical services personnel and bomb−squad members think, 'there's a better way to do this,' and we want to hear from them."
Source: http://www.dhs.gov/xnews/releases/pr_1175112507974.shtm

[Return to top]

Information Technology and Telecommunications Sector

26. *April 02, US−CERT* — **Technical Cyber Security Alert TA07−089A: Microsoft Windows ANI header stack buffer overflow.** A stack buffer overflow exists in the code that Microsoft

Windows uses to process animated cursor files. Specifically, Microsoft Windows fails to properly validate the size of an animated cursor file header supplied in animated cursor files. Animated cursor files can be included with HTML files. For instance, a web site can use an animated cursor file to specify the icon that the mouse pointer should use when hovering over a hyperlink. Because of this, malicious web pages and HTML email messages can be used to exploit this vulnerability. In addition, animated cursor files are automatically parsed by Windows Explorer when the containing folder is opened or the file is used as a cursor. Because of this, opening a folder that contains a specially crafted animated cursor file will also trigger this vulnerability. Note that Windows Explorer will process animated cursor files with several different file extensions, such as .ani, .cur, or .ico. Furthermore, Windows will automatically render animated cursor files referenced by HTML documents regardless of the animated cursor file extension. This vulnerability is actively being exploited and a fix is not currently available.
Additional reporting on the issue from the Internet Storm Center: http://isc.sans.org/
The latest workarounds are available from US−CERT here:
http://www.kb.cert.org/vuls/id/191609#solution
Microsoft advisory: http://www.microsoft.com/technet/security/advisory/935423.ms px
Source: http://www.us−cert.gov/cas/techalerts/TA07−089A.html

27. *March 30, InformationWeek* — **Worm attack masquerades as IE7 download offer.** A security company issued a warning Friday, March 30, about a widespread attack that's masquerading as an offer from Microsoft to download a version of Internet Explorer 7. The e−mails, which claim to come from admin@microsoft.com and have the subject line "Internet Explorer 7 Downloads," display an image that invites users to download beta 2 of Internet Explorer 7, according to an advisory from Sophos. Users who make the mistake of clicking on the link in the message, though, instead are infected by the W32/Grum−A worm. The Grum worm is an appender virus that infects executable files referenced by Run keys in the Windows Registry. When activated, it copies itself to \winlogon.exe and makes changes to the Registry. It also edits the HOSTS file, injecting a thread into system.dll and attempts to patch two system files.
Additional information: http://www.sophos.com/security/analyses/w32gruma.html
Source: http://www.informationweek.com/news/showArticle.jhtml;jsessionid=IBUSYRXOTJUUMQSNDLRCKHSCJUNN2JVN?articleID=198701553

28. *March 30, Computerworld* — **Pill spammers turn hackers to 'joe job' sites.** Spammers are hacking into legitimate Websites through unpatched vulnerabilities in the PHP scripting language to sidestep blacklists that block spam or bar access to known spammer sales sites, a security company said Thursday, March 29. The tactic, said Sophos PLC, is a form of "joe job" −− a term usually given to spam attacks expressly designed to blacken the reputation of a legitimate user or company. Here, though, the intention is to slip by antispam defenses. The spammers first hack a genuine site by exploiting any of several unpatched PHP bugs. Once inside a legitimate site's server, the spammer can set up a redirect so that specific traffic heading its way will be shunted to the junk mailer's selling site. Most of the spam, Cluley said, touts cheap pharmaceuticals. Last week, Canadian coroners said that a 57−year−old British Columbian woman, Marcia Bergeron, died from taking pills tainted with strontium and uranium. Bergeron had purchased the medications from an online pharmacy pretending to be based in Canada.
Source: http://www.computerworld.com/action/article.do?command=viewA

rticleBasic&articleId=9015195&intsrc=hm_list

29. *March 29, Federal Computer Week* — **Successful cyberattacks against DoD drop.** The number of successful cyberattacks against the Department of Defense (DoD) networks and information systems declined from about 130 in January 2005 to about 40 in January 2007, Air Force Lt. Gen. Charles Croom, director of the Defense Information Systems Agency, told a House Armed Services Committee subcommittee hearing March 28. In testimony to the House Terrorism, Unconventional Threats and Capabilities Subcommittee, Croom said the decline in successful attacks occurred at the same time DoD deterred increasingly larger numbers of attacks and probes against its information systems. The number of cyber incidents grew from 16,000 in 2004 to 23,000 in 2005 and 30,000 in 2006, he said, in addition to cyberscans running about four times that number each year.
Hearing information: http://www.house.gov/hasc/hearing_information.shtml
Transcript: http://armedservices.house.gov/pdfs/TUTC032807/Croom_Testimo ny032807.pdf
Source: http://www.fcw.com/article98089−03−29−07−Web

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

30. *March 31, Atlanta Journal Constitution* — **Three shot at Greenbriar Mall.** A security guard and two other people were shot Saturday, March 31, after at least four men attempted a brazen late afternoon robbery of a jewelry store in the Greenbriar Mall. The victims were taken to Grady Memorial Hospital. At least one of the wounded had critical, life−threatening injuries, said Atlanta, GA, police Officer Steve Coleman. The other two were in stable condition. Atlanta police Officer James Polite said four or five men attempted to rob Glitz Jewelers.
Source: http://www.ajc.com/metro/content/metro/atlanta/stories/2007/03/31/0331metshooting.html?imw=Y

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer